VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

School of Computer Science and Engineering
Fall Semester 2024-25
CAT I

SLOT: F1+TF1

Programme Name & Branch: B.Tech & CSE

Course Name & Code: Cyber Security-BCSE410L

Exam Duration: 90 Min. **Maximum Marks: 50**

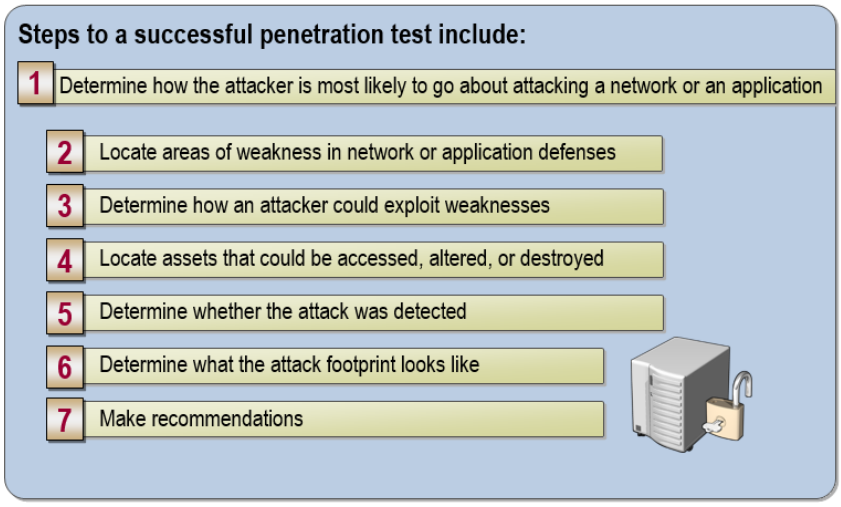
Q. No.	Question
1.	Identify the following attack and give solution for it. a. "The attacker does not allow to complete the TCP handshake by sending an ACK (acknowledge) packet back to the server". (3 Marks) b. "When an attacker tricks you to click a link that performs an unwanted action, such as transferring funds from your account." (3 Marks) c. When you give the value "OR 1=1" to the input field (4 Marks) a) TCP Attack. 1. Network Segmentation: 2. Intrusion Detection and Prevention Systems (IDPS): 3. Regular Patching and Updates: 4. Security Policies and Training: b) Cross-Site Request Forgery (CSRF) 1. Generating and Verifying Tokens: 2. Configuring SameSite Cookies: 3. Checking Headers: c) SQL Injection (SQLi) 1. Use Parameterized Queries (Prepared Statements) 2. Use Stored Procedures 3. Input Validation and Sanitization 4. Least Privilege Principle 5. Error Handling and Messages 6. Use ORM (Object-Relational Mapping) Libraries 7. Regular Security Audits and Code Reviews
2.	a. Explain the steps and components to successfully execute a security assessment principle (5 Marks)

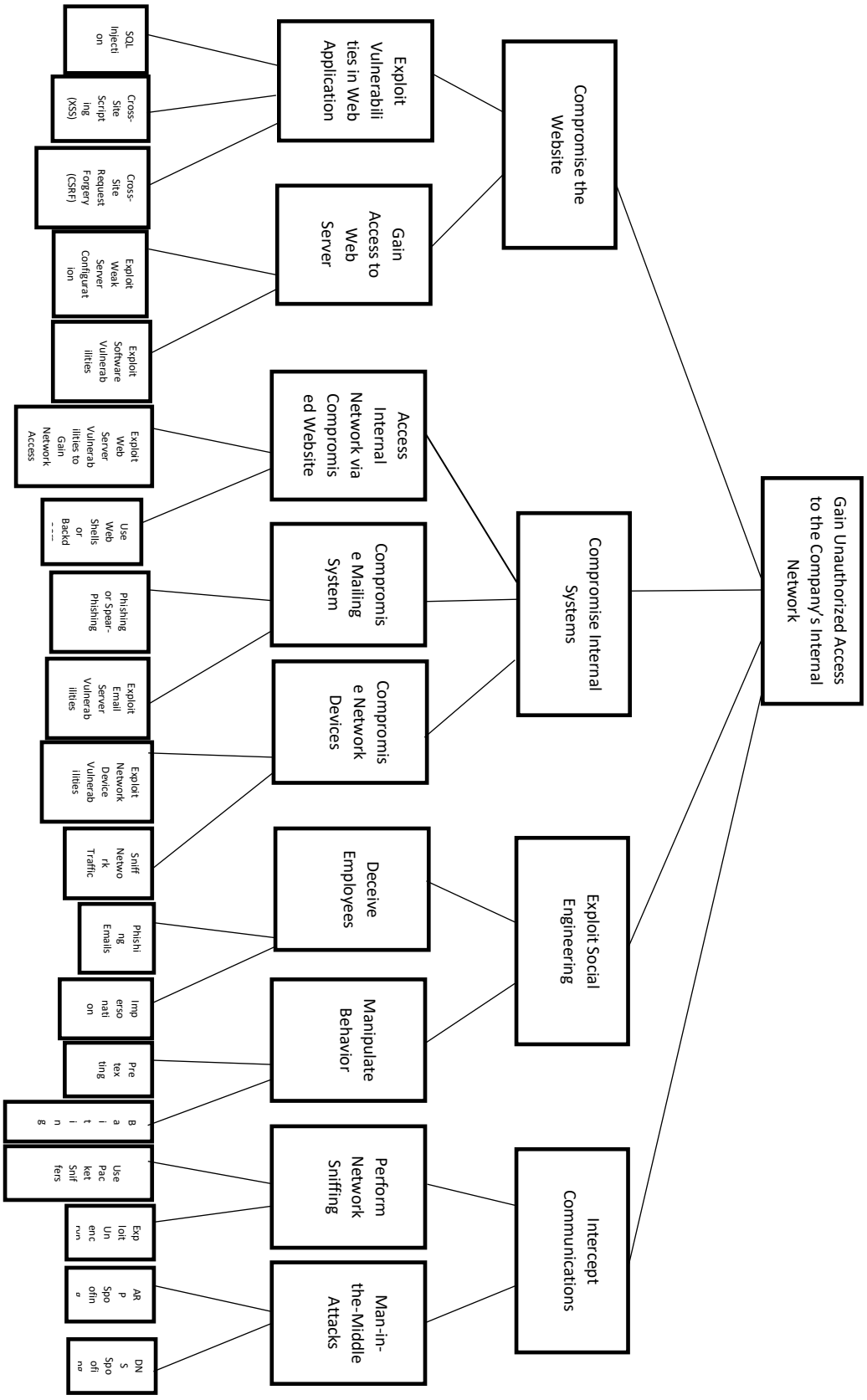
Project phase	Planning elements
Pre-assessment	• Scope • Goals • Timelines • Ground rules
Assessment	• Choose technologies • Perform assessment • Organize results
Preparing results	• Estimate risk presented by discovered weaknesses • Create a plan for remediation • Identify vulnerabilities that have not been remediated • Determine improvement in network security over time
Reporting your findings	• Create final report • Present your findings • Arrange for next assessment

Components of a Security Assessment

Components
Target
Target area
Timeline
Vulnerabilities to scan for

b. Describe the comprehensive phases of a penetration testing. (5 Marks)



3.	An attacker wants to gain unauthorized access to a company's internal network. To achieve that he plans to do the following: i. Compromise the Website ii. Compromise Internal Systems (Mailing system, Network) iii. Exploit Social Engineering iv. Intercept Communications. Assume you as the cyber security professional working on the same organization. Your role is to construct the Attack tree and analyze it to better understand the potential threats and develop a comprehensive security strategy to protect the organization. 

	Analysis and Security Strategy 1. Compromise the Website • Security Measures: o Secure Coding Practices: o Web Application Firewall (WAF): o Regular Patching: o Penetration Testing: 2. Compromise Internal Systems (Mailing System, Network) • Security Measures: o Network Segmentation: o Email Security: o Access Controls: o Intrusion Detection Systems (IDS): 3. Exploit Social Engineering • Security Measures: o Employee Training: o Simulated Phishing Tests: o Clear Reporting Channels: 4. Intercept Communications • Security Measures: o Encryption: o Network Monitoring: o Secure Protocols:
4.	a. Give example for the things that act as treasure in Dumpster diving and methods to prevent it. (4 Marks) **Dumpster diving** is a type of social engineering attack where attackers search through an organization's or individual's trash to find valuable information. Items found during dumpster diving can be used for identity theft, corporate espionage, or other malicious purposes. **Examples of Treasures in Dumpster Diving** 1. **Documents with Personal Information** o **Example**: Bank statements, medical records, or printed emails containing personal information such as names, addresses, phone numbers, Social Security numbers, or account details. 2. **Internal Corporate Information** o **Example**: Discarded meeting notes, strategic plans, financial reports, or sensitive business communications. 3. **Discarded Hardware** o **Example**: Old hard drives, USB drives, CDs, or DVDs that were not properly wiped. 4. **Access Badges or Security Cards** o **Example**: Discarded or lost employee ID cards, access badges, or key cards. 5. **Login Credentials or Passwords** o **Example**: Sticky notes or papers with written passwords, access codes, or PINs. **Methods to Prevent Dumpster Diving** 1. **Shred Documents** 2. **Secure Disposal of Electronic Devices** 3. **Use Locked Disposal Bins** 4. **Employee Training** 5. **Implement a Data Retention Policy**

b. Some best practices for your cyber security are listed below. For each practice list out two security threats that will arise if you fail to follow the practice. (6 Marks)

a. Avoid public Wi-Fi
b. Clean up your social media
c. Be wary of tempting offers.

a) Avoid Public Wi-Fi

Threat 1: Man-in-the-Middle (MitM) Attacks

Attackers can intercept the communication between your device and the internet, capturing sensitive data like login credentials, emails, and financial information.

Threat 2: Rogue Wi-Fi Hotspots

Attackers may set up fake Wi-Fi networks that look legitimate. Once connected, they can monitor your internet activity and steal your information.

b) Clean Up Your Social Media

Threat 1: Social Engineering Attacks

Attackers can gather personal information from your social media profiles to craft convincing phishing attacks, such as spear phishing, targeting you or your organization.

Threat 2: Identity Theft

Exposing too much personal information can lead to identity theft, where attackers use your details to open accounts, apply for loans, or commit other fraudulent activities in your name.

c) Be Wary of Tempting Offers

Threat 1: Phishing Scams

Tempting offers, such as "too good to be true" discounts or prizes, are often used as bait in phishing scams. Clicking on these links can lead to malicious websites designed to steal your personal information.

Threat 2: Malware Infections

Tempting offers can also be used to distribute malware. For example, downloading a "free" software offer might actually install malicious software on your device, compromising your data and security.

5. a. Complete the table given below (5 Marks)

S. No	Attack Scenario	Write Attack name	Write any two counter measures
1	When the perpetrators target your organization specifically and sends a fraud message pretending to come from a large and well-known company or website with a broad user base, such as Google or PayPal.	Spear Phishing	1. Email Filtering and Anti-Phishing Tools. 2. Employee Training and Awareness Programs
2	A type of cyberattack that specifically targets high-level executives (CEOs and CTOs) within an organization	Whaling	1. Executive-Level Security Awareness Training. 2. Enhanced Email and Communication Security

b. Write procedure to simulate any two Social Engineering attack using SEToolkit? (5 Marks)

Phishing Attack Simulation: Procedure**:**

1. **Start SEToolkit**:
2. **Select Attack Vector**:
    - When prompted, select the "Social-Engineering Attacks" option by typing the corresponding number and pressing Enter.
3. **Choose Phishing Attack**:
    - Choose "Website Attack Vectors" from the menu.
    - Then, select "Credential Harvester Attack Method" to create a phishing site that will capture credentials.
4. **Set Up the Fake Website**:
    - Select "Site Cloner" to clone a legitimate website that will be used to harvest credentials.
    - Enter the URL of the website you wish to clone (e.g., https://www.example.com).
5. **Configure the Listener**:
    - SEToolkit will prompt you to set up a local server that will host the cloned site. Configure the IP address and port as needed.
    - For phishing purposes, ensure you use a valid and reachable domain or IP for the fake site.
6. **Test the Phishing Page**:
    - After setup, verify that the cloned site is correctly hosted and reachable. Ensure that any credentials entered into the fake site are captured by SEToolkit.
7. **Deploy the Attack**:
    - Send a phishing email to the target (which should be done in a controlled and authorized environment for testing purposes). Include a link to the cloned site.
    - Ensure the targets understand this is a simulation and their data is handled responsibly.

2. Credential Harvesting Attack Simulation
Procedure:

1. **Select Attack Vector**:
    - Choose "Social-Engineering Attacks" from the main menu.
2. **Choose Credential Harvesting**:
    - Select "Website Attack Vectors".
    - Choose "Credential Harvester Attack Method".
3. **Select the Attack Type**:
    - Choose "Custom Import" if you want to design a custom page or "Site Cloner" if you want to clone an existing login page.
4. **Set Up the Fake Login Page**:
    - For "Custom Import," you'll need to provide the HTML file for the login page you want to use.
    - For "Site Cloner," enter the URL of a login page to clone, similar to the phishing attack setup.
5. **Configure the Listener**:
    - SEToolkit will ask you to configure the IP address and port for the server that will host the fake login page.
    - Ensure the server settings are correct and accessible.
6. **Verify and Deploy**:
    - Test the fake login page to make sure it is functioning correctly and capturing credentials.
    - Send out simulated phishing emails or messages with the link to the fake login page to the test subjects.
7. **Monitor and Analyze**:
    - Monitor the SEToolkit interface for captured credentials.
    - Ensure that all data is handled responsibly and that the test is conducted ethically.